

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-174955

(43)Date of publication of application : 02.07.1999

(51)Int.Cl.

G09C 1/00

(21)Application number : 09-347613

(71)Applicant : NIPPON TELEGR & TELEPH
CORP <NTT>

(22)Date of filing : 17.12.1997

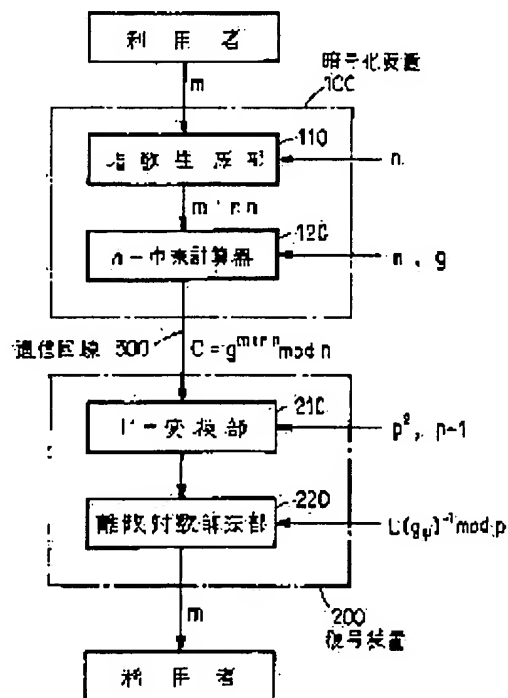
(72)Inventor : UCHIYAMA SHIGENORI
OKAMOTO TATSUAKI

(54) OPEN KEY CIPHERING DEVICE, OPEN KEY CIPHERING AND DECIPHERING
DEVICE, AND DECIPHERING PROGRAM RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To guarantee safety, to efficiently solve a discrete logarithmic problem, and to make the processing quantity the same as before.

SOLUTION: For add primes numbers (p) and (q), $n=p_2q$ and (g) is made open and (g) is selected out of $(Z/nZ)^*$ so that $g^p=gr-1 \bmod p_2$ has a location number (p) in $(Z/p_2Z)^*$; and $m+rn$ is found (110) from a plaintext (m) and a random number (r) and $C=gm+rn \bmod n$ is counted by using (n) and (g) to output a ciphertext (120). Then $C \bmod p_2$ is found for C, $(C^p-1)/p=L(C^p)$ is found, and a secret key $L(gp)-1 \bmod p$ is multiplied by $L(C^p)$ to obtain a plaintext (m) (200).



LEGAL STATUS

[Date of request for examination] 16.02.1999

[Date of sending the examiner's decision of
rejection]

[Kind of final disposal of application other than

the examiner's decision of rejection or
application converted registration]

[Date of final disposal for application]

[Patent number] 3402441

[Date of registration] 28.02.2003

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 特 許 公 報 (B 2)

(11) 特許番号

特許第3402441号
(P3402441)

(45) 発行日 平成15年 5 月 6 日 (2003. 5. 6)

(24) 登録日 平成15年 2 月 28 日 (2003. 2. 28)

(51) Int.Cl.⁷

G 0 9 C 1/00

識別記号

6 2 0

F I

G 0 9 C 1/00

6 2 0 A

請求項の数 8 (全 11 頁)

(21) 出願番号 特願平9-347613

(22) 出願日 平成9年12月17日 (1997. 12. 17)

(65) 公開番号 特開平11-174955

(43) 公開日 平成11年7月2日 (1999. 7. 2)

審査請求日 平成11年2月16日 (1999. 2. 16)

(73) 特許権者 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 内山 成憲

東京都新宿区西新宿三丁目19番2号 日

本電信電話株式会社内

(72) 発明者 岡本 龍明

東京都新宿区西新宿三丁目19番2号 日

本電信電話株式会社内

(74) 代理人 100066153

弁理士 草野 卓

審査官 中里 裕正

(56) 参考文献 特開 平5-181418 (J P, A)

現代暗号, 産業図書株式会社, 1997年

6月30日, p. 107-130

最終頁に続く

(54) 【発明の名称】 公開鍵暗号化装置、公開鍵暗号復号装置及び復号プログラム記録媒体

1

(57) 【特許請求の範囲】

【請求項1】 p 、 q を同一ビット数の奇素数として、
 $n = p^2 \cdot q$ を第1公開鍵とし、 n を法とする既約剰余類
群 $(\mathbb{Z}/n\mathbb{Z})^*$ の中から、 $g_0 = g^{p-1} \bmod p^2$ が
 $(\mathbb{Z}/p^2\mathbb{Z})^*$ の中での位数が p となる g を選んでそ
の g を第2公開鍵とし、

乱数 r と上記第1公開鍵 n を乗算し、その乗算結果に、
入力された平文を加算し指数を生成する指数生成手段
と、

上記第1公開鍵を法とした既約剰余類群において上記第
2公開鍵を上記指数で巾乗計算して暗号文を出力する巾
乗計算手段とを具備する公開鍵暗号化装置。

【請求項2】 p 、 q を同一ビット数の奇素数として、
 $n = p^2 \cdot q$ を第1公開鍵、 p を第1秘密鍵とし、 g_0 、
 n を法とする既約剰余類群 $(\mathbb{Z}/n\mathbb{Z})^*$ の元 C を0

2

$< g_0, C, < p^2$ の範囲にある整数で、 $g_0 \equiv C_0 \equiv$
 $1 \pmod{q}$ 、 $g_0 \not\equiv 1 \pmod{p^2}$ を満し、 $((g_0$
 $- 1) / p)^{-1} \bmod p$ を第2秘密鍵とし、

$0 < C < n$ の範囲にある整数で、 n と互いに素である入
力暗号文 C に対し、上記第1秘密鍵 p を用いて、 $C \bmod$
 $p^2 \in (\mathbb{Z}/p^2\mathbb{Z})^*$ を計算する p^2 - 還元手段と、
その p^2 - 還元手段の計算結果 $C \bmod p^2$ に対し p^2 を
法とする $p-1$ の巾乗計算を行って上記元 C を得る変
換手段と、

上記元 C を入力して $L(C) = (C_0 - 1) / p$ を
演算する対数計算手段と、

その演算結果 $L(C)$ と上記第2秘密鍵との積を上記
 p を法として求めて復号平文を出力する乗算手段とを具
備する公開鍵暗号復号装置。

【請求項3】 請求項1記載の公開鍵暗号化装置として

コンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項4】 請求項2記載の公開鍵暗号復号装置としてコンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項5】 p, q を素数とし、 $n = pq$ を第1公開鍵とし、 n を法とした剰余類環で定義される楕円曲線 E_p の点 G を第2公開鍵とし、

乱数 r に上記第1公開鍵を乗算し、その結果に入力平文 m を加算して指数を生成する指数生成手段と、

上記楕円曲線における巾乗計算を、上記指数を指数として上記第2公開鍵に対して行って暗号文を出力する巾乗計算手段とを具備する第2公開鍵暗号化装置。

【請求項6】 p を奇素数 (> 5)、 E_p を有限体 F_p 上の楕円曲線でその F_p 有理点の個数が p となるものとし、この F_p 有理点を G_p, C_p (どちらも無限遠点でない) とし、楕円曲線 $E_p(F_p)$ から有限体 F_p への写像関数を λ とし、 $\lambda(G_p)^{-1} \bmod p$ を秘密鍵とし、入力された暗号文 C を、上記 p を法として上記楕円曲線 $E_p(F_p)$ の元 C_p に変換する還元手段と、上記元 C_p と上記 p 、上記楕円曲線 E_p 、上記関数 λ を入力して $\lambda(C_p)$ を計算する対数計算手段と、上記 $\lambda(C_p)$ と、上記秘密鍵を入力して、両者の積を上記 p を法として求めて復号平文を出力する乗算手段とを具備する公開鍵暗号復号装置。

【請求項7】 請求項5に記載した公開鍵暗号化装置としてコンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項8】 請求項6に記載した公開鍵暗号復号装置としてコンピュータを機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は公開鍵暗号方式に用いる暗号装置、復号装置、その処理プログラムを記録した記録媒体に関する。

【0002】

【従来の技術】機密保持性のない通信回線を介してデータを送受信する場合、送受信のデータの盗聴防止に暗号法が用いられる。一般に、暗号法は共通鍵暗号と公開鍵暗号の二種類に区別できる。共通鍵暗号は暗号鍵と復号鍵が同じなので、鍵を秘密に配送する必要がある。また、通信の組合せ数と同じ数だけ鍵を必要とするので、ネットワーク内の送受信局数が増加すると、秘密に管理する鍵の数が急激に増加することが問題となる。

【0003】一方、公開鍵暗号は、暗号鍵と復号鍵が異なっており、暗号鍵を公開しても、暗号鍵から復号鍵を算出することが計算量的に難しければ、秘密鍵の秘密性は損なわれないので、暗号鍵の配送が不用である。また、各送受信局は自分の復号鍵だけを秘密に管理するの

で、秘密に管理する鍵の問題も解決できる。即ち、公開鍵暗号を利用すれば、共通鍵暗号を利用する時に問題であった鍵の管理の問題が解決される。また、共通鍵暗号を使う時の一番大きな問題であった、鍵配送の問題が解決出来る、即ち、鍵を秘密に配送する必要がない。また、共通鍵暗号では、鍵が当業者間で共有されているため、共通の鍵で作成された暗号文は、同鍵を所有する二人のうちいずれかが作成したかが特定することが出来ない。一方、公開鍵暗号では、秘密鍵を有するものが唯一であるため、同鍵で暗号化された文章を作成出来るのは、同鍵を持つもの唯一であるという意味で、証拠性を持ち得る。この性質を、デジタル署名と言う。

【0004】即ち、公開鍵暗号を用いれば、デジタル署名が実現出来、通信の相手を認証することに利用出来る。公開鍵暗号は、一方向性落し戸関数と呼ばれるものを使えば実現できることが知られている。一方向性関数とは、一方から他方への計算は簡単であるが、その逆を計算することは、計算量的に難しい関数のことで、その一方向性関数に「ある秘密を知っていれば、逆も簡単に計算できる」というしかけをもたせたものを一方向性落し戸関数と言い、そのしかけを「落し戸」と呼ぶ。現在のところ、素因数分解問題(合成数を入力とし、その合成数の素因子を出力する関数と、素因数分解することは同一視することが出来る。以下、IFPと表す。以下にあげる問題も、これと同様にある関数と同一視することが出来る)、有限体の乗法群における離散対数問題(例えば、 p を素数として、有限素体 F_p の乗法群 F_p^* = $\langle g \rangle$ において、その乗法群の元 y が与えられているとき、 $y = g^x$ なる、整数 x で $0 \leq x < p$ を満たすものを求める問題、以下、DLPと表す。)、有限体上の楕円曲線における離散対数問題(例えば、 p を素数として、有限素体 F_p 上定義された楕円曲線 $E(F_p)$ の有理点全体のなす群 $E(F_p)$ 、その一つの点 G 、点 G で生成される $E(F_p)$ の部分群の点 P が与えられている時、 $P = mG$ を満たす整数 m を求める問題、以下、ECDLPと表す、但し、 mG は、楕円曲線上の加法で G を m 倍した点を表す。楕円曲線、及び楕円曲線暗号に関しては、例えば、Menezes, A.J. 著 "Elliptic Curve Public Key Cryptosystems", Kluwer Academic Publishers (1993) を参照。以下、この文献を文献1と称す)などが、一方向性関数であろうと予想されているものの代表的なものであり、現在提案されている公開鍵暗号の中で、代表的かつ実用的なものは、RSA暗号、Rabin暗号、ElGamal暗号、楕円曲線暗号(楕円ElGamal暗号)が挙げられると思われるが、RSA暗号、Rabin暗号はIFPの難しさ、ElGamal暗号は、DLPの難しさ、楕円曲線暗号は、有限体上の楕円曲線の点のなす群におけるElGamal暗号で、これはECDLPの難しさに、それぞれ基づくものである。

【0005】RSA暗号については、Communication of

the ACM, vol.21, pp.120-126(1978)に、Rivest, R.L. 等によって、“A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”と題して論及されており（以下、この文献を文献2と称す）、Rabin 暗号については、MIT, Technical Report, MIT/LSC/TR-212(1979)にRabin, M.O.によって、“Digital Signatures and Public-Key Functions as intractable as Factorization”と題して論及されている（以下、この文献を文献3と称す）、さらに、ElGamal 暗号についてはIEEE Trans.on Information Theory, 1T-31, 4, p.469-472(1985)に、ElGamal T. によって、“A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”と題して論及されており（以下、この文献を文献4と称す）、楕円曲線暗号については、Miller, V. S. とKoblitz, N. によって、1985年に独立に提案されたものであるが、Proc.of Crypto'85, LNCS 218, Springer-Verlag, pp.417-426(1985)にMiller, V. S. によって“Use of Elliptic Curves in Cryptography”と題して論及され（以下、この文献を文献5と称す）、Math.Comp., 48, 177, pp.203-209(1987)にはKoblitz, N. によって“Elliptic Curve Cryptosystems”と題して論及されている（以下、この文献を文献6と称す）。

$$C \equiv E_1(M) \equiv M^e \pmod{n} \quad (1)$$

$$M \equiv D_1(C) \equiv C^d \pmod{n} \quad (2)$$

で定義する。この時、 M が $0 \leq M \leq n-1$ を満たすなら※

$$D_1(E_1(M)) = M \quad (3)$$

が成り立つ。

【0008】Rabin 暗号の構成法は次の通りである。

p, q, n を上述の通りに取り、さらに、 $0 \leq b \leq n$ を★

$$C \equiv E_2(M) \equiv M(M+b) \pmod{n} \quad (4)$$

$$M \equiv D_2(C) \equiv (-b \pm \sqrt{b^2 + 4C})/2 \pmod{p \text{ かつ } \pmod{q}} \quad (5)$$

で定義する。Rabin 暗号は、復号時に連立方程式を解くことになるが、二次方程式は二つの解を持つので、一般には四つの解が現れてきて、上のままでは復号が一意に出来ないという問題があった。これは、なんらかの付加的情報を付けて通信を行なう、即ち、運用上の問題として回避することも出来るし、一意に復号出来るように改良もされている。これに関しては、電子情報通信学会論文誌, Vol. J70-A, No. 11, pp.1632-1636(1987)

に、黒澤 馨等によって“素因数分解の困難さと同等の☆

$$C = (C_1, C_2) = E_3(M) \quad (6)$$

$$C_1 \equiv g^r \pmod{p} \quad (7)$$

$$C_2 \equiv y^r M \pmod{p} \quad (8)$$

$$M \equiv D_3(C) \equiv C_2 / C_1 \cdot x \pmod{p} \quad (9)$$

で定義する。ここで、 r は、 $0 < r < p$ なる任意の整数とし、暗号化処理をするたびに選ぶものとする。◆

$$M = D_4(E, (M)) \quad (10)$$

が成立する。楕円曲線暗号（楕円 ElGamal暗号）の構成は次の通りである。 p を素数、有限素体 F 。上の楕円曲線 $E(a, b): y^2 = x^3 + ax + b$ ($a, b \in F, 4a^3 + 27b^2 \neq 0$)、楕円曲線上の F 。一有理点 G で、その位数 q が十分大きな素数を約数に持つも*

$$C = (C_1, C_2) = E_4(M) \quad (11)$$

$$C_1 = rG, \quad (12)$$

ves in Cryptography”と題して論及され（以下、この文献を文献5と称す）、Math.Comp., 48, 177, pp.203-209(1987)にはKoblitz, N. によって“Elliptic Curve Cryptosystems”と題して論及されている（以下、この文献を文献6と称す）。

【0006】以下、具体的にこれらの暗号を紹介をし、その性質について述べる。RSA暗号の構成法は次の通りである。異なる奇素数 p, q を選び、 n, e, d を次の式を満たすように取る。

$$n = pq,$$

$$\text{GCD}(e, \text{LCM}(p-1, q-1)) = 1,$$

$$ed \equiv 1 \pmod{\text{LCM}(p-1, q-1)}$$

ここで、 $\text{GCD}(a, b)$ は、整数 a, b の最大公約数、 $\text{LCM}(a, b)$ は、整数 a, b の最小公倍数を表すものとする。

【0007】(n, e)を公開鍵(d, p, q)を秘密鍵として、暗号化処理(E_1)と復号処理(D_1)を

★満たす整数 b を取る。 (n, b) を公開鍵、 (p, q) を秘密鍵として、暗号化処理(E_2)、復号処理(D_2)を

☆強さを有する逆数を利用した公開鍵暗号”と題して論及されている。（以下、この文献を文献7と称する）

また、ElGamal 暗号の構成は次の通りである。 p を素数、 g を、 p を法とした既約剰余類群 $(\mathbb{Z}/p\mathbb{Z})^*$ の一つの生成元、即ち、位数が $p-1$ の元とし、 $0 < x < p$ なる整数 x を任意に取り、 $y \equiv g^x \pmod{p}$ とおく。この時、 (y, g, p) を公開鍵、 x を秘密鍵として、暗号化処理(E)、復号処理(D)を

◆【0009】 M が $0 < M < p$ であれば、

*のが取れるものとする。 $0 < x < q$ なる任意の整数を取り、 $E(a, b)$ 上の加法で $P = xG$ とする。この時、 $(p, E(a, b), G, P, q)$ を公開鍵、 x は秘密鍵として暗号化処理(E_4)、復号処理(D_4)を

7

$$C_2 = rP + M$$

$$M = D, (C) = (C_2 - xC_1, \text{の} X\text{-座標})$$

で定める。ここで、 r は $0 < r < q$ を満たす任意の整数とし、暗号化処理のたびに選ぶものとする。また、 $rP + M$ は、 X -座標が M となる楕円曲線上の点と点 rP との楕円曲線上での和を表すものとする。一般には、常に M を X -座標に持つ点が、与えられた楕円曲線上に存在するかどうかは分からないが（ここでの場合は、確率 $1/2$ で点が存在する）、何らかの、システムに共通の規則を定めて M にある程度の冗長情報を付加することによって、常に、冗長情報を付加したものを X -座標に持つような点が取れるように出来る。

【0010】次に、上述の暗号の計算量について述べる。RSA暗号の計算量は、暗号化処理、復号処理が共に k^3 のオーダーで実現されることが知られている。ここで、 k は公開鍵 n のビット数を表すとする。Rabin暗号の計算量は、暗号化処理は k^2 のオーダーで、復号処理は k^3 のオーダーで実現される。この k も公開鍵 n のビット数を表すものとする。

【0011】ElGamal暗号の計算量は、暗号化処理、復号処理共に k^3 のオーダーで実現できる。ここで、 k は、公開鍵である素数 p のビット数を表すものとする。さらに、楕円曲線暗号の計算量は、暗号化処理、復号処理共に k^3 のオーダーで実現できることが知られている。ここで、 k は公開鍵である素数 p のビット数であるとする。

【0012】オーダーで比較するなら、上述の暗号は計算量はあまり変わらないが、実装させると、差が出てくるとは明らかである。実際、楕円曲線上の加法は、その定義体である有限体における乗法の10倍程度時間がかかることが知られている。次に、安全性について述べる。暗号は、攻撃者（盗聴者）に通信内容を隠して送ることを目的とするため、どの程度通信内容を隠しているかの度合いが重要になる。即ち、秘匿性としては、完全解読（暗号文から、平文が完全に求められる事）と部分解読（暗号文から、平文の部分情報が求められる事）の二種類に分類できる。次に、公開鍵暗号の攻撃者のタイプには、単に暗号通信を受信し、その情報だけから解読を試みる受動的攻撃と、送信者に様々な質問とし（暗号文を送り）、その回答（その復号結果）をもらうことが許され、それらの情報をもとにして、目的とする暗号文を解読するような能動的攻撃の二種類に分けられる。特に、能動的攻撃の中でも、適応的選択暗号文攻撃（解読者が任意に選んだ暗号文を真の受信者に復号させた後、そこで得た情報と公開情報を用いて、別の暗号文を復号する攻撃）がもっとも強力である。

【0013】さて、そこで、これらの分類を元に、上述の代表的な公開鍵暗号の安全性について述べることにすると、RSA暗号、Rabin暗号のようなIFPの難しさに基づく暗号は、公開鍵 n を素因数分解出来れば、秘密

8

$$(13)$$

$$(14)$$

鍵である素数 p, q が分かり、 $LCM(p-1, q-1)$ が計算出来て、秘密鍵 d が求められ、安全に解読されてしまう、ここで、 $LCM(p-1, q-1)$ を、 n だけから求めようとするのは、 n を素因数分解することと等価であることが証明されている。即ち、 p, q が分からないままで、 $LCM(p-1, q-1)$ を求めることは出来ない。しかし、RSA暗号は、公開鍵 n を素因数分解する以外の方法で完全解読出来る可能性が残っているが、Rabin暗号を完全解読する方法は、公開鍵 n を素因数分解する以外にないことが証明されている。即ち、RSA暗号を解読することはIFPを解くことと等価であるかどうかは未解決であるが、Rabin暗号の完全解読は、IFPを解くことと等価であることが証明されている。（上述の逆数暗号も、IFPと等価であることが証明されている）このRabinの結果は、ある基本的な問題（今の場合、IFP）が難しいであろうと仮定することによって、暗号のある種の安全性が証明出来ることを初めて示したものである。今の場合、上述の公開鍵暗号の安全性で言えば、受動的攻撃に対して安全であることが、IFPの難しさを仮定した上で、証明されたことを意味している。部分解読に関しては、RSA暗号、Rabin暗号共に、暗号文 C から、平文 M の最下位ビットを求めることは、 C から、 M 全体を求めることと同じ位難しいことが証明されている。また、さらに同様に M の最下位より $\log k$ ビットの部分と同様の安全性を持つことが証明されている。この事実は、SIAM Journal of Computing, 17, 2, pp.449-457(1988)において、Alexi, W.等によって、“RSA and Rabin Functions: Certain Parts Are as Hard as the Whole”と題して論及されている。（以下、この文献を文献8と称す）

次に、ElGamal暗号の安全性についてであるが、これはDLPの難しさに基づく暗号であるので、DLPが解ければ、公開鍵 (y, g, p) から、秘密鍵 x が求められ、解読されてしまう。しかし、ElGamal暗号の解読がDLPと同じ程度に難しいかどうかは証明されていない。同様に、楕円曲線暗号についても、ECDLPと同じ程度に難しいかどうかは証明されていない。

【0014】以上、代表的かつ実用的な公開鍵暗号について説明したが、基本的な問題の難しさを仮定し、ある種の安全性が証明出来る公開鍵暗号は、Rabin暗号とその変形位しか知られていない。つまり、実用性を考えると、一方向性関数としてつかえるものは、IFP、DLPとECDLP位しか知られてなく、これらを使って新しい「落し戸」を作り、それを用いてある種の安全性の証明のついた新しい公開鍵暗号システムを作ることは一つの問題である。

【0015】

【発明が解決しようとする課題】上述のように、公開鍵

暗号は、従来からの共通鍵暗号と比較すれば、鍵管理の問題を解決することが出来、デジタル署名を実現することが出来るが、実用的な公開鍵暗号を実現するには、一方向性関数としてはIFP、DLPやECDLP位しか知られてなく、これらを用いて「落し戸」を作る作り方も本質的にこれ等位しか知られてなく、ましてや、ある種の安全性が証明されている暗号は、Rabin暗号とその変形だけである。

【0016】この発明の目的は、一方向性関数としてはIFPを用いながらも、新しい「落し戸」を用いて、IFPが難しいであろうという仮定に基づき、受動的攻撃に対して安全であることが証明できる公開鍵暗号装置を提供することである。

【0017】

【課題を解決するための手段】具体的には、この発明は二種類の公開鍵暗号装置を提供する。p、qを二つの素数として、 $n = p^2 \cdot q$ としたとき、nを法とした既約剰余類群 $(\mathbb{Z}/n\mathbb{Z})^*$ 上で構成されるものと、 $n = pq$ としたとき、nを法とした剰余類環 $\mathbb{Z}/n\mathbb{Z}$ 上で定義される楕円曲線E。上で構成される公開鍵暗号装置との二つを提供する。以下、前者を「乗法群に基づく公開鍵暗号装置」と呼び、後者を「楕円曲線に基づく公開鍵暗号装置」と呼ぶことにする。

【0018】有限素体F。上の楕円曲線で、位数がpのものをanomalous楕円曲線と呼ぶことにする。このano-

$$\Gamma = \{x \in (\mathbb{Z}/p^2\mathbb{Z})^* \mid x \equiv 1 \pmod{p}\} \quad (15)$$

$(\mathbb{Z}/p^2\mathbb{Z})^*$ における離散対数問題は、現在のところ、非常に難しい問題であると信じられていて、効率の良いアルゴリズムはまだ発見されていない、しかし、 Γ ※

$$L(x) = (x-1)/p, x \in \Gamma \quad (16)$$

この関数の値は、有限素体F。になるとみなせる。する★ ★と、この関数Lは、任意のa、b $\in \Gamma$ に対して

$$L(ab) = L(a) + L(b) \pmod{p} \quad (17)$$

なる性質を持つことが簡単に分かり、この関数は、 Γ からF。への群としての同型写像を与えていることも分かる。このLの計算量は、pのビット数をkとすれば k^2 のオーダーであることが簡単に分かる。従って、 Γ にお☆

$$L(y) = L(x^m) = mL(x) \pmod{p} \quad (18)$$

となるので、 $L(x) \neq 0 \pmod{p}$ であれば

$$m = L(y) / L(x) \pmod{p} \quad (19)$$

と、効率良く求めることが出来る。x、yから、mを求める計算量は、pのビット数をkとすれば、 k^3 のオーダーで出来る。

【0021】この性質を用いれば、全く新しい「落し

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/p^2\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^* \quad (20)$$

$$\simeq \Gamma \times (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^* \quad (21)$$

が成り立つので、「乗法群に基づく公開鍵暗号装置」は、以下で定められる： $g \in (\mathbb{Z}/n\mathbb{Z})^*$ で $g_0 = g^{p^{-1} \pmod{p^2}} \in \Gamma$ が $L(g_0) \neq 0 \pmod{p}$ を満たすものを取り、n、g、kを公開鍵とする。ここで、kは、素数※

$$C = g^{m+k \cdot n} \pmod{n} \quad (22)$$

*malous楕円曲線上の離散対数問題が非常に効率良く計算出来ることが、Smart,N.P.によって、“The Discrete Logarithm Problem on Elliptic Curves of Trace one, preprint(September,1997)”において(以下、この文献を文献9と称す)、佐藤考和等によって、“Fermat Quotient and the Polynomial Time Discrete Logarithm for Anomalous Elliptic Curves, preprint(September,1997)”において(以下、この文献を文献10と称す)、それぞれ独立に論及されている。このanomalous楕円曲線における離散対数問題を解くアルゴリズムを、以下ではSSAアルゴリズムと呼ぶことにする。

【0019】特に、後者の論文中で示唆されていることとして、ある種の群のp-Sylow部分群における離散対数問題が、非常に効率良く解けるという事実がある。ここで、p-Sylow部分群とは、例えば、有限群Hが与えられているとき、Hの部分群の中で、位数がpの巾となるものの中で最も位数が大きなものHのp-Sylow部分群という。この発明では、このある種の群のp-Sylow部分群における離散対数問題が非常に効率良く解けることを利用して、ある種の安全性の証明がつけられる、新しい公開鍵暗号を提供する。

【0020】pを奇素数として、 p^2 を法とした既約剰余類群 $(\mathbb{Z}/p^2\mathbb{Z})^*$ において、そのp-Sylow部分群 Γ 、即ち、この場合は位数pの部分群になるが、これは次のように書ける：

※における離散対数問題は非常に効率良く解ける。実際、次のような Γ 上定義された関数を考える：

☆ける離散対数問題、即ち、 $x \in \Gamma$ 、mを $0 < m < p$ から任意とり、 $y = x^m$ において、x、yからmを求める問題については、式(17)から

11

復号は、CをΓの元に変換することが出来れば、nの素因子pを知っているものは、上述の関数Lを用いて効率良くその離散対数を求めることが出来、mは $0 < m < 2^k$

$$C_0 = C^{p^{-1}} \bmod p^2$$

とすれば、 $C_0 \in \Gamma$ となり、上記L関数を用いて離散対数を効率的に解くことができる。また、この公開鍵暗号を解読することは、公開鍵nを素因数分解することと、即ち、MIFPと等価であることが証明できる。

【0022】この発明の「乗法群に基づく公開鍵暗号装置」においては、暗号化装置は、平文と乱数を組み合わせて、法nで巾乗計算のための指数部分を生成する指数生成部、mod nでの巾乗計算を行う、n-巾乗計算部からなり、n-巾乗計算部で生成された暗号文を通信回線※

$$E_0 : y^2 = x^3 + a_0 x + b_0$$

$$(a_0, b_0 \in F_p, 4a_0^3 + 27b_0^2 \neq 0), \quad (24)$$

$$E_1 : y^2 = x^3 + a_1 x + b_1$$

$$(a_1, b_1 \in F_q, 4a_1^3 + 27b_1^2 \neq 0), \quad (25)$$

$a = a_0 \bmod p, b = b_0 \bmod p, a = a_1 \bmod q, b = b_1 \bmod q$ なるa、bは、中国人剰余定理よりmod n★

$$E_n : y^2 = x^3 + ax + b \quad (a, b \in \mathbb{Z}/n\mathbb{Z}, \text{GCD}(4a^3 + 27b^2, n) = 1) \quad (26)$$

を得る。以下、特別にことわらない限りは、上述のよう★ ☆に中国人剰余定理を用いて得られる関係にあるものは

$$E_n = \{E_0, E_1\}, a = \{a_0, a_1\}, b = \{b_0, b_1\} \quad (27)$$

などと表すことにする。また、特に、法を強調したいと◆ ◆きは

$$E_n = \{E_0 \bmod p, E_1 \bmod q\} \quad (28)$$

などともあらわすことにする。

【0024】今、 E_0 はanomalous楕円曲線、 E_1 はanomalousでない楕円曲線とする。このとき、上述の「乗法群に基づく公開鍵暗号装置」と同様にn、 E_n 、 E_n ($\mathbb{Z}/n\mathbb{Z}$)の点G、kを公開鍵としておく。但し、 $G \neq 0$

$$C = (m + rn)G \in E_n(\mathbb{Z}/n\mathbb{Z}) \quad (29)$$

復号は、nの素因子pを知っているものは、この暗号文の定義式をmod pとして、 $E_0(F_p)$ の点の間の関係式に変換することが出来るので、上述のSSAアルゴリズムを用いて効率良くその離散対数を求めることが出来、したがって効率良く復号が出来る。また、この公開鍵暗号を解読することは、公開鍵nとanomalous楕円曲線とanomalousでない楕円曲線から中国人剰余定理を用いて得られる $\mathbb{Z}/n\mathbb{Z}$ 上の楕円曲線 E_n 、点Gが与えられたとき、これから、nを素因数分解することと等価であることが証明できる。即ち、このn、 E_n と、その曲線上の点Gが与えられたとき、nを素因数分解する問題を、変形素因数分解問題（以下では、MIFPと表すことにする）と呼ぶことにすると、この楕円曲線 E_n を用いた暗号を解読することは、MIFPと等価であることが証明できる。

【0025】この発明の「楕円曲線に基づく公開鍵暗号装置」においては、暗号化装置は、平文と乱数を組み合わせて、 $E_n(\mathbb{Z}/n\mathbb{Z})$ における巾乗計算のための指数部分を生成する指数生成部、 $E_n(\mathbb{Z}/n\mathbb{Z})$ での巾

12

2^{k-1} の範囲にあるので、mod pでは一意に定まり、したがって、効率良く復号が出来る。CをΓの元に変換する方法は、

(23)

※に送出する。一方、復号装置は、法 p^2 での $p-1$ 乗計算を行う、Γ-変換部とΓにおける離散対数問題を解いて復号する、離散対数解法部からなる。

【0023】次に、この発明の「楕円曲線に基づく公開鍵暗号装置」について述べる。これに対しても同様に、二つの素数p、qを取り、 $n = pq$ とし、 F_p 、 F_q 上の楕円曲線 E_0 、 E_1 がそれぞれ次で与えられているとする：

★で一意に定まり、 $\mathbb{Z}/n\mathbb{Z}$ 上で定義された楕円曲線

※は十分大きな（例えばビット数がnと同じ）位数を持つものとしておき、kは、素数p、qのビット数とする。このとき、平文mを $0 < m < 2^{k-1}$ から取ることにすると、rを $\mathbb{Z}/n\mathbb{Z}$ から任意に取り、暗号化を次で定める

乗計算を行う、 E_n 巾乗計算部からなり、 E_n 巾乗計算部で生成された暗号文を通信回線に送出する。一方、復号装置は、 $E_n(\mathbb{Z}/n\mathbb{Z})$ の点を $E_0(F_p)$ の点に変換するmod p-還元器と、 $E_0(F_p)$ における離散対数問題を解いて復号する、SSAアルゴリズム部からなる。

【0026】

【発明の実施の形態】はじめに、この発明による「乗法群に基づく公開鍵暗号装置」、「楕円曲線に基づく公開鍵暗号装置」それぞれの基本は機能構成を述べ、後に、それぞれの各部における一実施例について説明する。まずは、「乗法群に基づく公開鍵暗号装置」について、

(1) 鍵の生成

奇素数p、qを任意に選び、 $n = p^2 q$ とする。ただし、p、qのビット数は同じでkとする。また、 $\text{GCD}(p, q-1) = 1$ を満たしているとする。

【0027】さらに、gを $(\mathbb{Z}/n\mathbb{Z})^*$ の中から、 $g = g^{p^{-1}} \bmod p^2$ が $(\mathbb{Z}/p^2\mathbb{Z})^*$ の中での位数がpとなるものを取る。すると、上述の関数LでL

$(g_0) \neq 0 \bmod p$ が成立する。実際、 $(Z/p^2 Z)^*$ の中で位数が p となるものは $1 + k p \bmod p^2$ (k は p で割れない) と表せ、したがって $L(1 + k p) = ((1 + k p) - 1) / p = k \neq 0 \bmod p$ となるからである。また、具体的に、 g を生成する方法としては、ランダムに g を $(Z/nZ)^*$ から選ぶと、 $L(g_0) \neq 0 \bmod p$ となる確率は $1 - (1/p)$ 程度と考えられるので、無視出来ない確率で選ぶことが出来る。利用者は、公開は出来ないが、システムパラメータの一つとして $L(g_0)^{-1} \bmod p$ をあらかじめ計算しておくことに*10

$$C = g^{m+r^n} \bmod n$$

(3) 復号処理

暗号文 C の定義式 (30) の両辺を、それぞれ $p-1$ 乗すると、 $\bmod n$ での合同式は、勿論、 $\bmod p^2$ でも成立 ※

$$C^{p-1} = g^{(p-1)(m+r^n)} = g_0^m \times g_0^{r^n \bmod p^2} = g_0^m \bmod p^2$$

(30)

従って

$$C_0 = C^{p-1} \bmod p^2$$

(32)

とおけば

$$C_0 = g_0^m \bmod p^2$$

(33)

$C_0, g_0 \in \Gamma$ であるから、上述で定義した関数 L を使★ ★うと

$$L(C_0) = L(g_0^m) = mL(g_0) \bmod p$$

(34)

即ち

$$m = L(C_0) / L(g_0) \bmod p$$

(35)

となり、復号出来る。

【0030】従って、復号処理を整理すると、まず、暗号文 C に対して、式 (32) で C_0 を計算し、次に $L(C_0)$ を計算し、最後に $L(C_0)$ と、あらかじめ計算しておくことが出来る $L(g_0)^{-1} \bmod p$ との $\bmod p$ での積を取って復号出来る。

(3) 「乗法群に基づく公開鍵暗号装置」が、受動的攻撃に対して安全であることの証明。

【0031】「乗法群に基づく公開鍵暗号装置」を解読することと、 n を素因数分解することが同値であることを示す。 n を無視できない確率で素因数分解するアルゴリズムが存在すれば、明らかに「乗法群に基づく公開鍵暗号装置」を解読する平均的多項式時間アルゴリズムが構成できるので、ここでは、次の事実のみを証明する：

“「乗法群に基づく公開鍵暗号装置」を無視できない確率で解読するアルゴリズム A 存在するならば、 n を素因数分解する平均的多項式時間アルゴリズムを構成出来る” (ここで、上述の “ n を無視できない確率で素因数分解するアルゴリズム” という意味は、そのアルゴリズムを入力 n のビット数の多項式オーダー程度繰り返し適用することによって、かならず素因数分解出来るアルゴリズムのことである。以下、同様の使い方をする。厳密な定義は、文献 11 を参照)

実際、今、合成数 $n (= p^2 \cdot q)$ が与えられているとすると、ランダムに $g \in (Z/nZ)^*$ を選んで、この発明の公開鍵暗号装置のパラメータとして、無視できない

*する。

【0028】従って、 (n, g, k) を公開鍵 (p, q) を秘密鍵とする。ここで $L(g_0)^{-1} \bmod p$ も秘密鍵と考えて良い。

(2) 暗号化処理

平文 m (但し、 $0 < m < 2^{k-1}$) に対して、まず、乱数 r を $0 \leq r < n$ の範囲から選び、 $m + r n$ を計算し、暗号文 C は以下のように計算する。

【0029】

※し、 $g_0 \bmod p^2$ の位数は p であり、 $r n$ は p の倍数であって $g_0^{r n} = 1$ となるから、

確率でとることが出来て、次に、 x を Z/nZ からランダムに選ぶとき、 $x \bmod p \text{ LCM}(p-1, q-1)$ の分布と、この発明の公開鍵暗号装置における、暗号化処理時の途中の計算に出てくる、 $m + r n$ に対する、 $m + r n \bmod p \text{ LCM}(p-1, q-1)$ の分布の差は、無視できる確率であることが証明できる。従って、 Z/nZ からランダムに x を選び、 $C = g^x \bmod n$ で計算された C は、無視できない確率で暗号文だと、アルゴリズム A は認識し、 C に対応する平文 x_0 を出力する。今、 x が、 $x < 2^{k-1}$ なる範囲の数となる確率は無視できるので、無視できない確率で $x \geq 2^{k-1}$ としてよく、すると、 $x \equiv x_0 \pmod{p}$ 、また、 $x_0 < 2^{k-1}$ より、 $x \equiv x_0 \pmod{n}$ が不成立となり、したがって、 $\text{GCD}(x - x_0, n)$ を計算すると、この値は $p, p q, p^2$ のいずれかとなり、 n を素因数分解することが出来る。全体として、 n のビット数の平均的多項式時間で素因数分解出来る。つまり n を素因数分解することと同値であって、受動的攻撃に対する安全性が高い。

【0032】次に、「楕円曲線に基づく公開鍵暗号装置」について、暗号の構成法、及び、変形素因数分解問題と等価であることについて述べる。まず最初に、復号に利用する SSA アルゴリズムについて述べる。有限素体 F 。上の anomalous 楕円曲線 E 上の離散対数問題とは、その F 。-有理点 G, P が与えられたとき、 $P = m G$ となる $m \in Z/pZ$ を求めることであるが、SSA アルゴリズムは、上でも述べたが、anomalous 楕円曲線上

の離散対数問題の解法を与えるアルゴリズムで、有限素体 F_p 上の anomalous 楕円曲線であれば、 p のビット数を k として、計算量は k^3 のオーダーである効率的なアルゴリズムであって、具体的には次のような手順となる：

SSAアルゴリズム

入力：(G, P, E)

出力： m

手順1 E を Z 上に持ち上げた楕円曲線 E' で、 $E(F_p)$ から F_p への写像 $\lambda_{E'}$ が、自明な写像にならないものを選ぶ。これは、 p のビット数を k とすれば、 k^3 のオーダーで計算できる。

手順2 手順1で構成した写像 $\lambda_{E'}$ を使って $\lambda_{E'}$ (G)、 $\lambda_{E'}$ (P) を計算し (これは k^3 のオーダー＊

$$E_p: y^2 = x^3 + a_p x + b_p,$$

$$(a_p, b_p \in F_p, 4a_p^3 + 27b_p^2 \neq 0), \quad (36)$$

$$E_{p'}: y^2 = x^3 + a_{p'} x + b_{p'},$$

$$(a_{p'}, b_{p'} \in F_{p'}, 4a_{p'}^3 + 27b_{p'}^2 \neq 0), \quad (37)$$

但し、 $\#E_p(F_p) = p$ 、 $\#E_{p'}(F_{p'}) = p' = q$ 、 $+1-t(-2\sqrt{q} \leq t \leq 2\sqrt{q}, t \neq 1, q' \neq p)$ を満たすとする。 $\#$ は集合の元 (要素) の数を表わす。期待する位数を持つ楕円曲線の構成方法は、虚数乗法論を援用した比較的効率の良い生成方法が提案されていて、特に、anomalous 楕円曲線の生成については、例えば、IEICE Trans. Fundamentals, E76-A, 1, pp. 50-54 (1993) において、“Elliptic Curve Suitable for Cryptography” と題して、Miyaji, A. により論及されている。

$$E_n: y^2 = x^3 + ax + b (a, b \in Z/nZ, \gcd(4a^3 + 27b^2, n) = 1)$$

$$(38)$$

すなわち、すでに定義した記号で書けば

$$E_n = [E_p, E_{p'}], \quad a = [a_p, a_{p'}], \quad b = [b_p, b_{p'}] \quad (39)$$

である。また

$$G = [G_p, G_{p'}]$$

$$(40)$$

としておく。

【0033】さらに、SSAアルゴリズムを用いて、公開はせずに、システムパラメータの一つとしてあらかじめ $\lambda_{E_n}(G_p)^{-1} \bmod p$ を計算しておく。これも秘密鍵の一つとして考えて良い。以下、簡単のために、この写像を λ と書く。従って、 (n, E_n, G, k) を公開鍵、 (p, q) を秘密鍵とする。ここで、 $E_p, E_{p'}, \star$

$$C = (m + rn)G \in E_n (Z/nZ)$$

$$(41)$$

但し、これは、楕円曲線 E_n 上の加法を用いて、点 G を $m + rn$ 倍したものであって、暗号文が楕円曲線上の点であることに注意。すなわち、二つの Z/nZ の元の組である。(あえて書けば、 $C = (Cx, Cy)$ 、 $Cx, Cy \in Z/nZ$)

☆

$$C_p = (m + rn)G_p = mG_p \in E_p(F_p)$$

$$(42)$$

なる、anomalous 楕円曲線における離散対数問題に変換される。ここで、 $C = [C_p, C_{p'}]$ とおいた。

◆【0035】従って SSA アルゴリズムを用いて m は求められる。実際、 λ の準同型性により、

$$\lambda(C_p) = \lambda(mG_p) = m\lambda(G_p) \bmod p$$

$$(43)$$

即ち

＊で出来る)、 $m = \lambda_{E'}(P) / \lambda_{E'}(G) \bmod p$ を計算する (これは、 k^3 のオーダーで出来る)

いずれにしても、 p のビット数を k とすれば、SSA アルゴリズムの計算量は k^3 のオーダーである。この $\lambda_{E'}$ は、 $E(F_p)$ から F_p への群としての同型写像をあたえる。なお、 $\lambda_{E'}$ の構成方法など、詳しくは、文献10を参照。また p が5以下であれば SSA アルゴリズムを用いることなく効率的に解ける。

(1) 鍵の生成

奇素数 p, q を任意に選び、 $n = pq$ とする。ただし、 p, q のビット数は同じで k とする。次に、 F_p 上の anomalous 楕円曲線 E_p 、 $F_{p'}$ 上の anomalous でない楕円曲線 $E_{p'}$ を選ぶ：

※ (以下、この文献を文献12と称す) さらに、 $E_p(F_p), E_{p'}(F_{p'})$ 各々の点 $G_p, G_{p'}$ で、位数が $\text{ord}(G_p) = p, \text{ord}(G_{p'}) = q'$ なるものを選びと仮定する。ここで、 $E_p(F_p)$ は、一般には巡回群になるとは限らないが、ここでは簡単のためこう仮定しておく。一般には、 q' が十分大きな素因子をもつようなものにし、その大きな素数を位数とする点を $G_{p'}$ と取って良い。次に、中国人剰余定理を使って、 Z/nZ 上の楕円曲線 E_n を作る：

★ $G_p, G_{p'}, \lambda(G_p)^{-1} \bmod p$ も秘密鍵と考えてもよい。

(2) 暗号化処理

平文 m (但し、 $0 < m < 2^{k-1}$) に対して、まず、乱数 r を $0 \leq r < n$ の範囲から選び、 $m + rn$ を計算し、暗号文 C は以下のように計算する。

【0034】

☆ (3) 復号処理

暗号文 C の定義式 (41) の両辺を、それぞれ $\bmod p$ とすると、 rn は p の倍数であって $rnG \bmod p = 0$ となるから、

$$m = \lambda(C_0) / \lambda(G_0) \bmod p$$

となり、復号出来る。

【0036】従って、復号処理を整理すると、まず、暗号文Cに対して、 $C = C_0 \bmod p$ を計算し、次に $\lambda(C_0)$ を計算し、最後に $\lambda(C_0)$ と、あらかじめ計算しておくことが出来る $\lambda(G_0)^{-1} \bmod p$ との $\bmod p$ での積を取って復号出来る。

(3)「楕円曲線に基づく公開鍵暗号装置」が、受動的攻撃に対して安全であることの証明。「楕円曲線に基づく公開鍵暗号装置」を解読することと、公開鍵 (n, E_0, G, k) という情報から n を素因数分解することが同値であることを示す。即ち、変形素因数分解問題と同値であることを示す。

【0037】 n を無視できない確率で素因数分解するアルゴリズムが存在すれば、明らかに「楕円曲線に基づく公開鍵暗号装置」を解読する平均的多項式時間アルゴリズムが構成できるので、ここでは、次の事実のみを証明する：“「楕円曲線に基づく公開鍵暗号装置」を無視できない確率で解読するアルゴリズムB存在するならば、 n を素因数分解する平均的多項式時間アルゴリズムを構成出来る”（ここで、上述の“ n を無視できない確率で素因数分解するアルゴリズム”という意味は、そのアルゴリズムを入力 n のビット数の多項式オーダー程度繰り返し適用することによって、かならず素因数分解出来るアルゴリズムのことである。以下、同様の使い方をする。厳密な定義は、文献11を参照）

実際、今、合成数 $n (=pq)$ が与えられているとすると、 z を $\mathbb{Z}/n\mathbb{Z}$ からランダムに選ぶとき、 $z \bmod LCM(p-1, q-1)$ の分布と、我々の公開鍵暗号システムにおける、暗号化処理時の途中の計算に出てくる、 $m + rn$ に対する、 $m + rn \bmod pq'$ の分布の差は、無視できる確率であることが証明できる。従って、 $\mathbb{Z}/n\mathbb{Z}$ からランダムに z を選び、 $C = zG \in E_0$ ($\mathbb{Z}/n\mathbb{Z}$)で計算された C は、無視できない確率で暗号文だと、アルゴリズムBは認識し、 C に対する平文 z を出力する。今、 z が、 $z < 2^{k-1}$ なる範囲の数となる確率は無視できるので、無視できない確率で $z \geq 2^{k-1}$ としてよく、すると、 $z \equiv z_0 \pmod{p}$ 、また、 $z_0 < 2^{k-1}$ より、 $z \equiv z_0 \pmod{n}$ が不成立となり、したがって、 $GCD(z - z_0, n)$ を計算すると、この値は p となり、 n を素因数分解することが出来る。全体として、 n のビット数の平均的多項式時間で素因数分解出来る。

【0038】次に、この発明の「乗法群における公開鍵暗号装置」、「楕円曲線に基づく公開鍵暗号装置」それぞれの、実施例について説明する。まずは、「乗法群における公開鍵暗号装置」の一実施例について説明する。図1に示すように、暗号装置100と復号装置200が通信回線300により接続されている。暗号化装置100は、指数生成部110と法 n での巾乗計算器120を

有す。復号装置200は、 Γ -変換器210と離散対数解法部220を有する。

【0039】まず、暗号化装置100での暗号化処理について説明する。暗号化装置100における指数生成部110の詳細を図に示す。指数生成部110は、暗号化装置100の利用者から平文(m)を受けると、乱数生成器111は乱数 $r \in \mathbb{Z}/n\mathbb{Z}$ を発生させ、これを乗算器112に入力して、 rn を計算し、これを加算器113に入力して $m + rn$ を計算し、この結果を n -巾乗計算器120に入力して、暗号文 $C = g^{m+rn} \bmod n$ を生成する。

【0040】次に、復号装置200での復号処理について説明する。復号装置200における Γ -変換器210の詳細を図2Bに示す。また、離散対数解法部220の詳細を図4に示す。復号装置200における Γ -変換部210は、通信回線300から、暗号文(C)を受けると、 $\bmod p^2$ -還元器211で $C \bmod p^2$ を計算し、この値を Γ -変換器212に入力して、 $C_0 = C^{p^{-1}} \bmod p^2$ を計算し、 C_0 を離散対数解法部220に入力する。離散対数解法部220は、 Γ -変換部210から C_0 を受けると、それを、対数計算機221に入力し、 $L(C_0)$ を計算する。次に、これを、乗算器222に入力し $L(C_0) \times L(g)^{-1} \bmod p$ を計算する。この値を、離散対数解法部220は復号平文 m として出力する。

【0041】次は、「楕円曲線に基づく公開鍵暗号装置」の一実施例について説明する。図3にこの発明の一実施例を示す。暗号装置400と復号装置500が通信回線600により接続されている。暗号化装置400は、指数生成部410と E_0 -巾乗計算器420を有す。復号装置500は、 $\bmod p$ -還元器510とSSAアルゴリズム部520を有する。

【0042】まず、暗号化装置400での暗号化処理について説明する。暗号化装置400における指数生成部410の詳細を図4Aに示す。指数生成部410は、暗号化装置400の利用者から平文(m)を受けると、乱数生成器411は乱数 $r \in \mathbb{Z}/n\mathbb{Z}$ を発生させ、これを乗算器412に入力して、 rn を計算し、これを加算器413に入力して $m + rn$ を計算し、この結果を E_0 -巾乗計算器420に入力して、暗号文 $C = (m + rn)G$ を生成する。

【0043】次に、復号装置500での復号処理について説明する。復号装置500におけるSSAアルゴリズム部520の詳細を図4Bに示す。復号装置500における $\bmod p$ -還元器510は、通信回線600から、暗号文(C)を受けると、 $C_0 = C \bmod p \in E_0(F_0)$ を計算し、 C_0 をSSAアルゴリズム部520に入力する。SSAアルゴリズム部520は、 $\bmod p$ -還元器510から C_0 を受けると、それを、対数計

算機521に入力し、 $\lambda(C_0)$ を計算する。次に、これを、乗算器522に入力し $\lambda(C_0) \times \lambda(G_0)^{-1} \bmod p$ を計算する。この値を、SSAアルゴリズム部520は復号平文 m として出力する。

【0044】

【発明の効果】以上説明したように、この発明によれば、素因数分解問題の困難さを仮定した上で、ある種の安全性の証明のついた、今までにない新しい公開鍵暗号システムを構成することが出来る。従って、現在では n が1024ビット程度であれば、 n を素因数に分解することは現実的には困難であるから、 n を1024ビット程度以上にしておけば十分安全なものとなる。

【0045】暗号化処理、復号処理の計算量は共に、 k^3 のオーダーであって、現在までに知られている代表的な公開鍵暗号と比べても同程度であり、非常に実用的な暗号であるとも言える。さらに、受動的攻撃に対する安全性が証明されているため、現在もっとも有力と考えら*

【図1】

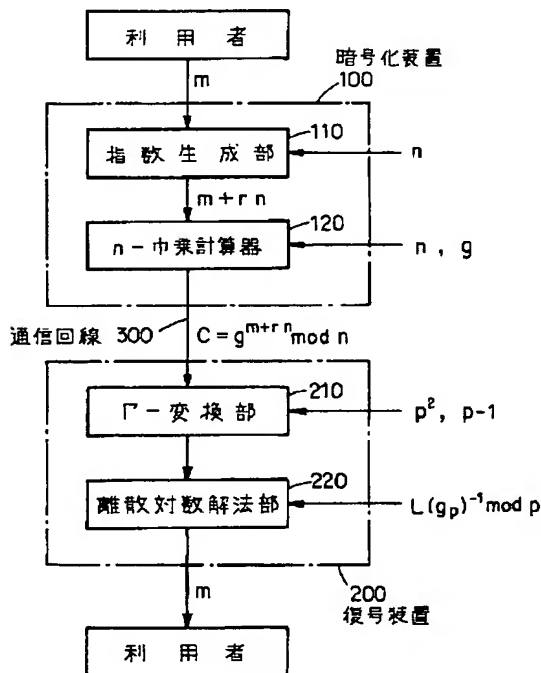


図 1

*れているRSA暗号よりも安全なことが保証される。

【図面の簡単な説明】

【図1】この発明の「乗法群に基づく公開鍵暗号装置」における暗号装置と復号装置の一実施例の機能構成を示すブロック図。

【図2】Aは図1中の指数生成部110の具体的機能構成例を示すブロック図、Bは図1中の Γ -変換部210の具体的機能構成例を示すブロック図、Cは図1中の離散対数解法部220の具体的機能構成例を示すブロック図である。

【図3】この発明の「楕円曲線に基づく公開鍵暗号装置」における暗号装置及び復号装置の各実施例の機能構成を示すブロック図。

【図4】Aは図3中の指数生成部410の具体的機能構成例を示すブロック図、Bは図3中のSSAアルゴリズム部520の具体的機能構成例を示すブロック図である。

【図2】

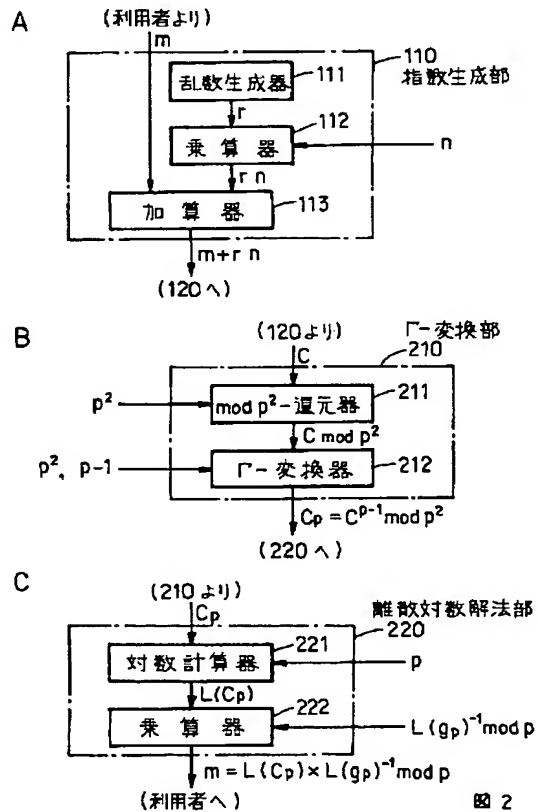


図 2

【図3】

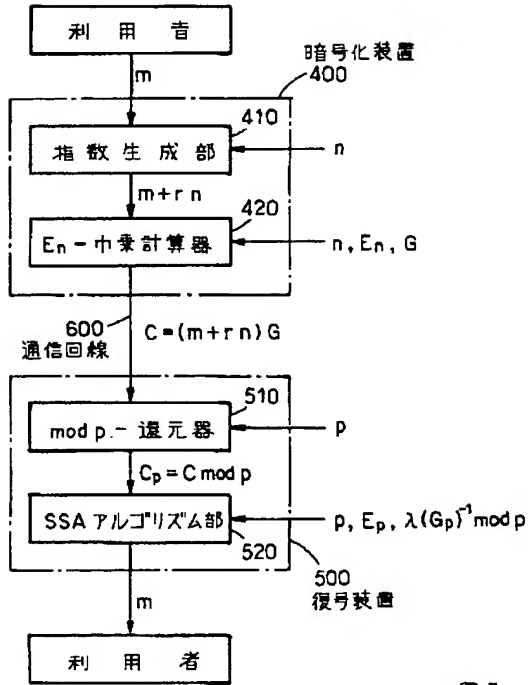


図 3

【図4】

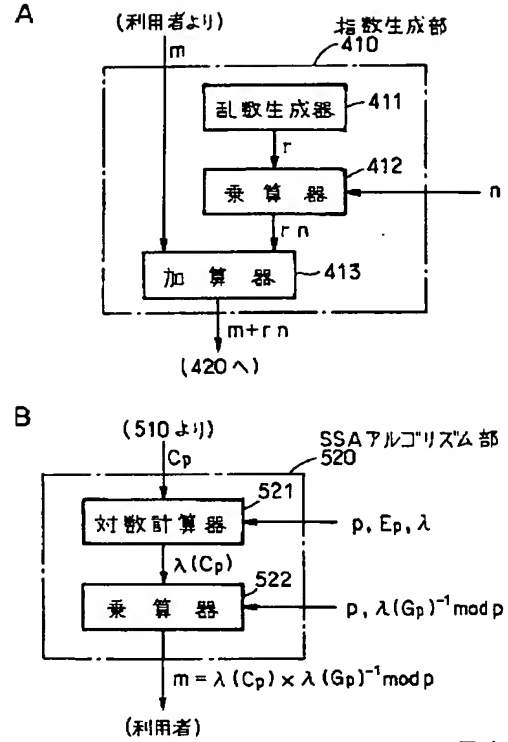


図 4

フロントページの続き

(58)調査した分野(Int.Cl.⁷, DB名)

G09C 1/00 620

JICSTファイル(JOIS)